

WEST CHESTER UNIVERSITY POLICY ON ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES AND SYSTEMS BY EMPLOYEES

- I. **PURPOSE:** The purpose of this policy is to establish parameters of acceptability for use of the University computing facilities and resources by University employee account-holders.
- II. **DEFINITIONS:**
 - A. **Acceptable Use:** For use to be acceptable, it must demonstrate awareness and sensitivity towards the intent of the University in granting users access, the co-existing privileges of other users, the rights of others to privacy and freedom from harassment or annoyance, the intellectual property rights of others, and the ownership and confidentiality of data.
- III. **POLICY:**
 - A. **General Policy:** Access to the University's computing and information network facilities and resources is a privilege granted solely to the University's faculty, staff, students and those other individuals who have been approved for special accounts. The intent of the University in granting access to individuals is to support the academic mission of the University, to share information and ideas and to manage its administrative and service operations and activities. Obtaining and maintaining an electronic account is a privilege, not a right. All users must show responsibility and proper judgment, as well as comport with the framework of acceptability in order to maintain the integrity of these facilities and resources for all users. While the University respects the individual's right to free speech and free expression, it is expected that the use of the system will fall within the guidelines of generally accepted social standards of the University and demonstrate respect for all members of the campus community. The University reserves the right to limit or revoke electronic account privileges for misuse or abuse of those privileges. Agreement to abide by this policy is a condition of acceptance to use the University's computing and information network facilities and resources.
 - B. **Specific Policy Considerations:**
 1. **Protecting Data:** The information of the University is one of its most valuable assets. Information must be safeguarded for reasons of data integrity, confidentiality, **availability** and privacy. The following rules must be observed:
 - a. Never share a password with another person.
 - b. Never attempt to discover or use another individual's password or network ID.

- c. **Never attempt to circumvent data protection schemes or uncover security loopholes.**
- d. **Never attempt to monitor another user's data communications, or attempt to read, copy, change, delete or transmit another's user files or software.**
- e. **Never attempt to gain unauthorized access to remote computers.**
- f. **Always protect data **media (diskettes, Flash drives, DVDs, etc.)** by securing them immediately after use.**
- g. **Always back-up data regularly.**

2. **E-Mail**: University e-mail account-holders can generally expect that the content of e-mail files residing in their user accounts will be treated as confidential by the University. The University does not routinely examine these files or monitor their content. Under certain circumstances, however, e-mail can lose its confidentiality. It can be lost if the University is compelled by court order to be released, by signed release from the user, if the files are transmitted by the user to others and user custody is lost, or when such information is deemed by University officials to be of evidenciary interest to a disciplinary investigation. Under these specific circumstances, e-mail privacy cannot be guaranteed by the University. Users should be cognizant of the lack of expectation of privacy under these circumstances. The following rules must be observed:

- a. **Never send or forward chain mail.**
- b. **Do not open or execute attachments which appear suspect. Attachments are a popular way of distributing viruses.**
- c. **Never use your account for personal business purposes.**
- d. **Never send harassing, annoying, threatening, defamatory, offensive or fraudulent messages or images to others.**
- e. **Always think before sending e-mail, especially if angry or upset. E-mail is difficult to retrieve at best and is never retrievable if already opened by the receiving party.**
- f. **Always delete e-mail which does not require preservation.**
- g. **Always remember that when the confidentiality of a message is critical, there is no substitute for face-to-face communication.**
- h. **Always remember that e-mail messages which are sent can easily be forwarded or redistributed to others. Custody lost is an open door to privacy lost.**

- 3. Ownership and Use of Computing and Information Technology Facilities and Resources:** University information technology facilities and resources may be acquired by the University through lease, purchase, license, loan or other agreement. Facilities and resources may include computers, work stations, peripherals, networks, communication devices, switches, software programs and systems, as well as related devices and hardware and telecommunications equipment. Ownership lies with the institution, not the user. The University has established the following rules associated with the use of its computing and information technology facilities and resources. They must be observed:
- a. Never run or install a program which could result in damage to or destruction of a data file, computer system or information network. The willful introduction of viruses, worms and Trojan horses are expressly prohibited.
 - b. Never be wasteful of computing or information network resources or unfairly monopolize these resources. Waste in the form of examples such as unauthorized mass mailings, chain mail, unnecessary printing output, or creating unnecessary network traffic are expressly prohibited.
 - c. Never attempt to modify a program or diskette which the University supplies for use.
 - d. Never engage in behavior which could impair or impact the operation of computers, terminals, peripherals or networks. Acts such as tampering with the LAN, the high-speed backbone network, or otherwise blocking communication lines or interfering with the operational readiness of a computer is expressly prohibited.
 - e. Never use the University's computers, workstations or information networks for financial gain or other personal benefit, or for other reasons which result in a direct cost to the University.
 - f. Never abuse work time by spending large amounts of time at work in pursuit of social or other non-related personal interests which engage the use of the University's computing and information technology facilities and resources. (Examples of this form of inappropriate use include chat rooms, sexually explicit sites, sports fantasy and betting sites, etc.)
 - g. Never store or attempt to download or otherwise transmit data which would constitute a violation of state or federal law or the policies of the University, the State System of Higher Education or the Commonwealth of PA.
 - h. Always abide by the terms of all software licensing agreements. Unauthorized copying of software is expressly prohibited.

IV. PROCEDURES:

- A. **Minor Infractions:** Frequently, the IT Security Administrator will be able to manage a minor violation by contacting the employee, advising them of the violation, working through a solution and obtaining employee assurance that it will not happen again.
- B. **Investigating Alleged Serious Misuse of Computing and Information Technology Facilities and Resources:**
1. **Investigations:** Unfortunately, from time to time computer abuse, e-mail harassment, other unauthorized acts do occur. When they occur, they must be effectively managed to avoid recurrences. Everyone has a responsibility to report these types of acts if witnessed or suspected. Given such notice, the University has an obligation to investigate misuse of computing and information technology facilities and resources, including e-mail abuse.
 - a. **Reporting Suspected Misuse or Other Violation of this Policy:** Instances of alleged misuse/violation should be reported to the University's IT Help-Desk immediately. The Help-Desk will determine either to make an effort to resolve the situation or, if necessary, refer the concern to the IT Security Administrator for further review and action.
 - b. **Additional Notifications:** Anytime employee misconduct is alleged, the Director of Human Resources and the Department Director must be notified immediately by the IT Security Administrator. If the allegation might reasonably lead to a criminal complaint, the Human Resources Director will notify the Director of Public Safety immediately. If the allegation relates to possible sexual harassment or another form of illegal discrimination, the Human Resources Director will notify the Social Equity Director immediately. Notice to the employee who is the subject of the investigation shall be made by the appropriate University official after consultation with the Director of Human Resources.
 - c. **Decision to Investigate:** The IT Security Administrator, in consultation with the Human Resources Director and other appropriate University officials, will review the concern and determine how to best approach the conduct of a thorough investigation prior to investigatory action being undertaken.
 - d. **Privacy Interests:** Every reasonable effort will be made by the IT security administrator and any others involved in an investigation pursuant to this policy to balance a minimization of intrusion upon employee privacy interests while responsibly conducting a complete investigation. SSHE legal counsel will be consulted if questions arise in this regard.
 - e. **Collective Bargaining Agreements:** The Director of Human Resources will be consulted regarding employee collective bargaining rights relating to investigations and pre-disciplinary

meetings if the subject of a complaint is a member of a collective bargaining unit.

f. **Suspension of User Privileges:** There may be circumstances where the nature of an allegation is so serious as to require a suspension of privileges while an investigation is being conducted. Under these circumstances, both the employee and the union (where applicable), will be notified at the time of the suspension. Suspension of user privileges pending the outcome of an investigation is not a disciplinary action.

C. **Disciplinary Consequences:** Verified, serious misuse or repeated, minor infractions of this policy will result in disciplinary action. The typical form of disciplinary action for noncriminal offenses is loss or restriction of privileges, although other forms of discipline which would be more appropriate under the circumstances are possible. Under normal circumstances, disciplinary actions will be issued by the department director or by the University official charged with that responsibility as part of the collective bargaining relationship.

D. **Criminal Offenses:** Knowingly engaging in a scheme or artifice, including but not limited to a denial of service attack upon a computer, computer system, computer network, computer software, computer program, computer server, computer database, World Wide Web site or telecommunication device or any part thereof is a 3^d degree felony punishable by fine or imprisonment. (18 Pa.C.S. 3933) Sexual exploitation of children via the Internet is also a 2nd degree felony under PA law. (18 Pa.C.S. 6320)

* **Note:** Employees are advised to seek clarification of any aspects of this policy which are unclear to them before questionable acts are undertaken. Employees who have questions should contact the University's IT Help Desk.